# Communiqué de Presse

www.pandasecurity.com/france

## Plus de 10 millions de personnes dans le monde ont été exposées au risque de vol d'identité en 2008

- **Une étude de PandaLabs révèle des taux alarmants d'infection par des menaces informatiques servant à usurper l'identité des utilisateurs.**

- **Le nombre de PC infectés par ce type de menaces a augmenté de 800 % entre le deuxième et le quatrième trimestre 2008**

Paris, le 19 mars 2009

Panda Security, éditeur leader de solutions de sécurité, rend public les résultats de l'enquête sur le vol d'identité réalisée par PandaLabs, le laboratoire de détection et d'analyse des malwares de l'entreprise. A partir de l'analyse de 67 millions d'ordinateurs en 2008, PandaLabs a révélé que 1,1% des utilisateurs d'Internet dans le monde ont été exposé à des codes malveillants actifs susceptibles de dérober leur identité. A partir des résultats d'ActiveScan, le service d'analyse en ligne de Panda Security, PandaLabs a estimé que plus de 10 millions d'Internautes dans le monde étaient infectés l'année dernière par des malwares actifs capables de dérober leur identité.[1]

Selon une étude récente publiée par un cabinet de recherche indépendant, le coût moyen du vol d'identité aux États-Unis est de 496 $ pour chaque victime, ce qui ramène le coût total de l'usurpation d'identité rien que dans ce pays à 1,5 million de dollars.[2]

Principales conclusions de l'enquête de PandaLabs sur l'usurpation d'identité sur Internet :

- 1,07% de tous les PC analysés en 2008 étaient infectés par des malwares actifs (c'est-à-dire des malwares résidents en mémoire lors de l'analyse) liés au vol d'identité, par exemple des chevaux de Troie bancaires.
- 35 % des PC infectés avaient un logiciel antivirus installé et à jour.
- Le nombre de PC infectés par des malwares conçus pour dérober l'identité des utilisateurs a augmenté de 800 % entre le premier et le deuxième semestre 2008.
- PandaLabs prévoit une augmentation mensuelle du taux d'infection de 336 % au cours de l'année 2009, d'après la tendance observée les 14 mois précédents.

Des malwares actifs sont des codes malveillants qui sont chargés en mémoire et en exécution sur l'ordinateur au moment de l'analyse. Les utilisateurs infectés par ce type de menaces qui utilisent des services en ligne (achats sur Internet, banque en ligne, réseaux sociaux, ...) ont été victime d'usurpation d'identité sous une forme ou une autre. Selon la FTC (Federal Trade Commission), les victimes consacrent en moyenne 30 heures à résoudre chaque incident.[3] En mettant en parallèle ce chiffre et le taux d'infection estimé par Panda Security, les pertes liées au vol d'identité atteignent plus de 90 millions d'heures perdues, en plus du coût financier.

L'étude a révélé un autre fait inquiétant : 35 % des PC infectés par ce type de malwares étaient équipés de logiciels antivirus à jour. Les laboratoires antivirus reçoivent chaque jour un grand nombre de nouveaux codes malveillants à analyser (30.000 nouveaux échantillons par jour selon les données de PandaLabs). Les

---

[1] Chiffre obtenu à partir du nombre estimé d'utilisateurs d'Internet dans le monde en 2008 : 1 milliard (222.141.961 aux États-Unis). Source: http://www.internetworldstats.com

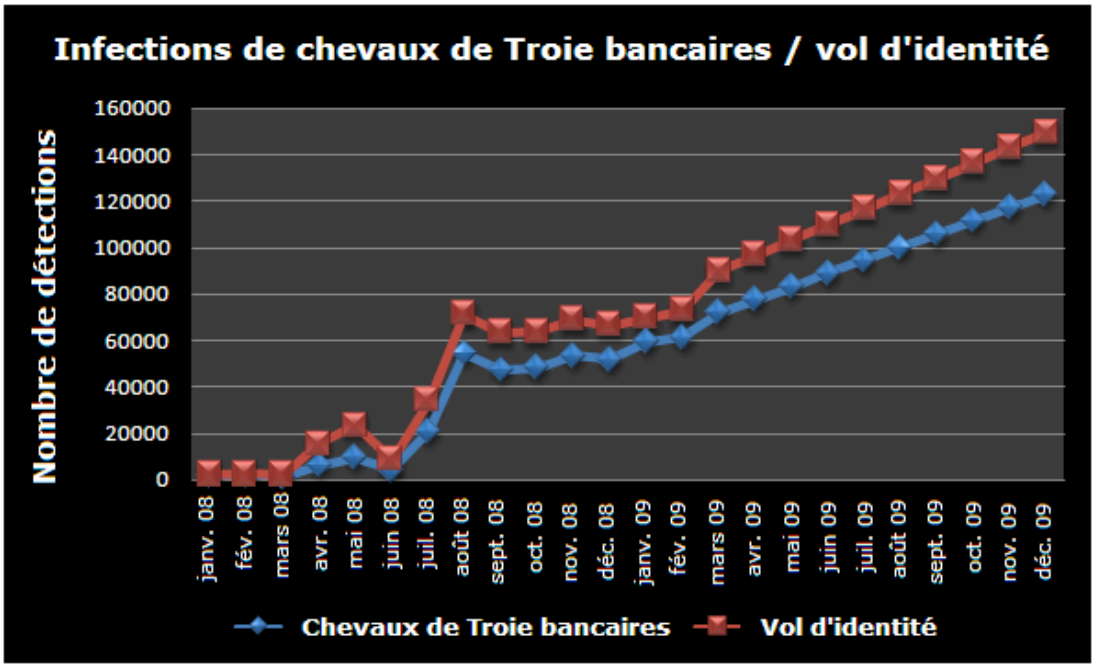
[2] 2009 Identity Fraud Survey Report: Identity Fraud on the Rise But Consumer Costs Plummet as Protections Increase http://www.javelinstrategy.com/

[3] http://www.consumer.gov/idtheft/pdf/ftc_06.16.05.pdf

éditeurs antivirus  doivent ainsi mettre à jour en permanence leurs services pour faire face au volume sans cesse croissant des nouvelles menaces. Des laboratoires tels que PandaLabs ont réalisé des avancées importantes dans l'automatisation de la détection et la classification des menaces. Ces nouvelles méthodes de détection ainsi que l'amélioration des techniques de surveillance et la détection via Internet ont réduit les risques de vol d'identité et les pertes associées. Certaines banques dans le monde, au Brésil entre autres, ont modifié les techniques d'authentification à leurs services en ligne, avec l'utilisation de jetons électroniques et de claviers virtuels. Ces approches mettent cependant du temps à être adoptées dans tous les pays, notamment aux États-Unis.

« Nous nous attendons à une croissance mensuelle de 336 % des codes malveillants visant à usurper l'identité des Internautes en 2009, une hausse portée par les gains considérables que les cybercriminels génèrent avec cette activité », explique Luis Corrons, le directeur technique de PandaLabs. « Il est important que les utilisateurs prennent conscience du risque de vol d'identité et se protègent contre les pertes potentielles que cette menace représente, tant au niveau financier que des pertes de temps. »

Le tableau ci-dessous présente la croissance et la corrélation entre les infections de chevaux de Troie bancaires et le vol d'identité entre janvier 2008 et février 2009 ainsi que les prévisions de croissance de PandaLabs pour le reste de l'année.

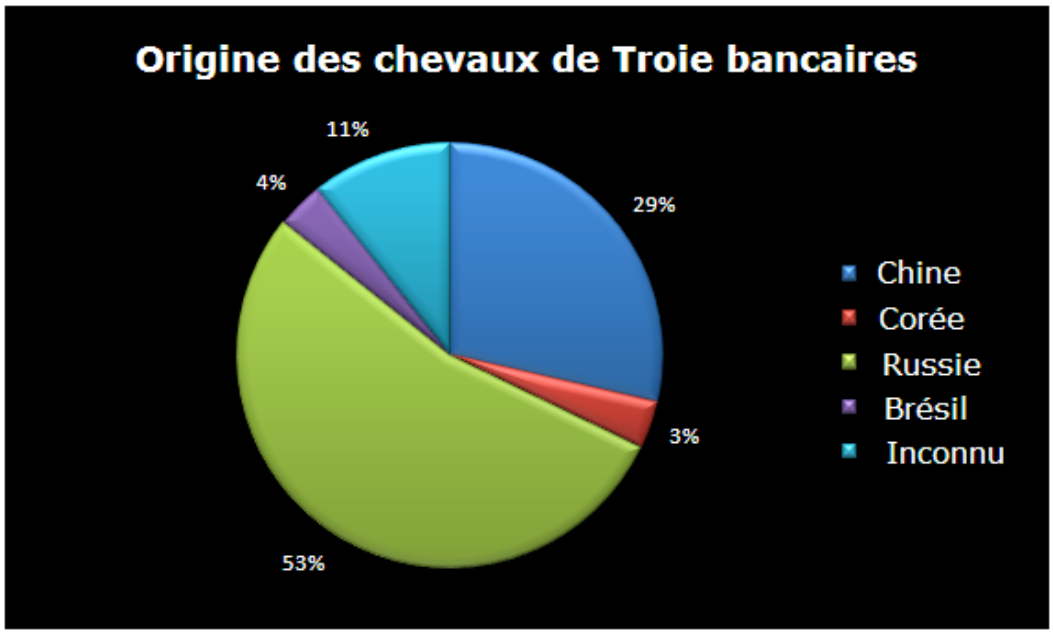



Les chevaux de Troie bancaires sont un type de malwares conçus spécifiquement pour dérober les informations des comptes bancaires auprès des banques et de leurs clients. Ces chevaux de Troie sont de plus en plus sophistiqués et peuvent maintenant se mettre à jour et étendre la liste des banques attaquées via Internet. Selon PandaLabs, les familles de chevaux de Troie bancaires les plus présentes sur les systèmes infectés sont les suivantes :

Trj/Cimuz
Trj/Sinowal
Trj/Bankolimb
Trj/Torpig
Trj/Goldun
Trj/Dumador
Trj/Spyforms
Trj/Bandiv
Trj/SilentBanker

Trj/PowerGrabber
Trj/Bankpatch
Trj/Briz
Trj/Snatch
Trj/Nuklus
Trj/Banker

Ces chevaux de Troie bancaires proviennent principalement de Chine et de Russie mais également de plus de plus de Corée et du Brésil. Le tableau ci-dessous présente l'origine de ces chevaux de Troie.




En dehors des chevaux de Troie bancaires, d'autres menaces informatiques servent à usurper l'identité des utilisateurs, par exemples des malwares conçus pour dérober les noms d'utilisateurs et mots de passe de chat, jeux et applications ou d'autres informations personnelles. Ces autres menaces les plus courantes sont les suivantes :

Trj/Lineage
W32/Lineage.worm
Trj/Legmir
Trj/Wow
W32/Wow.worm
Trj/MSNPassword
Trj/PassStealer
Trj/QQPass

Pour plus d'informations sur les chevaux de Troie bancaires, consultez le blog de PandaLabs à l'adresse : http://pandalabs.pandasecurity.com/archive/Bank-details-uncovered.aspx (en anglais).

**A propos de PandaLabs**

Depuis 1990, la mission de PandaLabs est d'analyser les nouvelles menaces le plus rapidement possible pour assurer une totale sécurité à nos clients. Pour cela, PandaLabs a développé un système automatisé et innovant qui analyse et traite les milliers de nouveaux échantillons reçus chaque jour et renvoie automatiquement un verdict (logiciel malveillant ou inoffensif). Ce système repose sur l'Intelligence Collective

Antimalware, le nouveau modèle de sécurité de Panda Security, qui détecte même les codes malveillants capables de passer au travers des autres solutions de sécurité.

Actuellement, 94 % des malwares détectés par PandaLabs sont analysés par l'Intelligence Collective Antimalware. Cette analyse automatique est complétée par le travail de plusieurs équipes spécialisées dans chaque type spécifique de malware (virus, vers, chevaux de Troie, logiciels espions, phishing, spam, rootkits, etc.) qui travaillent 24 heures sur 24 et 7 jours sur 7 pour offrir une garantie maximale. Grâce à ce système, Panda peut offrir à ses clients des solutions plus sûres, plus simples et consommant moins de ressources.

Pour plus d'informations, visitez le blog de PandaLabs : http://www.pandalabs.com et le site Web de Panda Security : www.pandasecurity.com/france.


| | | |
|---|---|---|
| | ATTACHEE DE PRESSE :<br>ÉMILIE SACKSICK<br>**SACKSICK@ELIOTROPE.FR**<br>LIGNE DIRECTE : **01 53 17 16 43** | **ELIOTROPE**<br>151, rue du Faubourg Saint Antoine<br>75011 Paris France<br>**www.eliotrope.fr**<br>TEL : + 33 (0)1 53 17 16 40<br>FAX : + 33 (0)1 53 17 16 41 |